10-02-00

A

Please type a plus sign (+) inside this box → ⊞

PTO/SB/05 (08-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S Patent and Trademark Office; U S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	Bilicska 3-2
First Inventor	Carl Bilicska
Title	AUTOMATED AUTHENTICATION HANDLING
Express Mail Label No.	EJ692288349US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☑ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. □ Applicant claims small entity status.
See 37 CFR 1.27.
3. ☑ Specification [*Total Pages* 12]
(preferred arrangement set forth below)
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (*if filed*)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☑ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 4]
5. Oath or Declaration [*Total Pages* 9]
   a. ☑ Newly executed (original or copy)
   b. □ Copy from a prior application (37 CFR 1.63 (d))
   (for continuation/divisional with Box 17 completed)
      i. □ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b)
6. □ Application Data Sheet. See 37 CFR 1.76

7. □ CD-ROM or CD-R in duplicate, large table or Computer Program (*Appendix*)
8. Nucleotide and/or Amino Acid Sequence Submission
(*if applicable, all necessary*)
   a. □ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. □ CD-ROM or CD-R (2 copies); or
      ii. □ paper
   c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☑ Assignment Papers (cover sheet & document(s))
10. □ 37 CFR 3.73(b) Statement *(when there is an assignee)* ☑ Power of Attorney
11. □ English Translation Document *(if applicable)*
12. □ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations
13. □ Preliminary Amendment
14. ☑ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
15. □ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. □ Other: ....
....

17. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No.:________________/__________________

Prior application information *Examiner*______________________ *Group / Art Unit* ______________________________

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

18. CORRESPONDENCE ADDRESS

□ *Customer Number or Bar Code Label* (Insert Customer No. or Attach bar code label here) or ☑ *Correspondence address below*

Name	Donald J. Cox, Jr.				
Address	Gibbons, Del Deo, Dolan, Griffinger & Vecchione 1 Riverfront Plaza				
City	Newark	State	NJ	Zip Code	07102-5497
Country	USA	Telephone	973-596-4853	Fax	973-639-6368

Name (Print/Type)	Donald J. Cox, Jr.	Registration No. (Attorney/Agent)	37, 804
Signature		Date	September 29, 2000

Burden Hour Statement. This form is estimated to take 0.2 hours to complete Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

PTO/SB/17 (08-00)
Approved for use through 10/31/2002 OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 730.00

Complete if Known	
Application Number	Bilicska et al.
Filing Date	September 29, 2000
First Named Inventor	Carl Bilicska
Examiner Name	Unassigned
Group Art Unit	Unassigned
Attorney Docket No.	Bilicska 3-2

METHOD OF PAYMENT (check one)

1. ☑ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 12-2325

Deposit Account Name: Lucent Technologies, Inc.

□ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

□ Applicant claims small entity status. See 37 CFR 1.27

2. □ **Payment Enclosed:**
□ Check □ Credit card □ Money Order □ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility filing fee	
106	310	206	155	Design filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 690.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims	13	-20** =	0	X	0	=	0
Independent Claims	2	- 3** =	0	X	0	=	0
Multiple Dependent					0	=	0

***or number previously paid, if greater; For Reissues, see below*

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim, if not paid
109	78	209	39	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	380	216	190	Extension for reply within second month	
117	870	217	435	Extension for reply within third month	
118	1,360	218	680	Extension for reply within fourth month	
128	1,850	228	925	Extension for reply within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,210	241	605	Petition to revive - unintentional	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	690	246	345	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	690	249	345	For each additional invention to be examined (37 CFR § 1.129(b))	
179	690	279	345	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) ______________________________

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY				Complete *(if applicable)*	
Name (Print/Type)	Donald J. Cox, Jr.	Registration No. (Attorney/Agent)	37,804	Telephone	973-596-4853
Signature				Date	09/29/2000

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Express Mail No.: EJ692288349US

PATENT
Bilicska 3-2

AUTOMATED AUTHENTICATION HANDLING SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to an automated authentication handling system. More particularly, the present invention relates to automating the authentication of a client among multiple servers.

2. Description of the Related Art

With the advent of networked computing systems, the user's need to use information and services distributed across computer networks and, in particular, the Internet has grown. In many instances, access to remote services and applications is restricted and requires an authentication process by the user before access is provided. As many more services are provided on such networks, the task of providing a separate authentication for each service can become burdensome to the end user. This can be especially true when the services are related in tasks or ownership.

Figure 1 illustrates a conventional configuration wherein clients 22-24 are connected to a network 26. A plurality of application servers 28-30 each having an authentication engine 32 are also connected to the network 26. Communication to these application servers by the clients, shown for purposes of illustration by lines 34-36 requires that the clients first establish a communications link with the application server 28-30 and then interact with the respective authentication engines 32 to establish access to the application server. In some instances establishing a trusted communication link meant that clients co-located at a facility were dedicated to communicate with a selected application server. Users wishing to use different applications had to physically move from client to client when wishing to access different application servers.

Figure 2 illustrates another configuration wherein the clients 22-24 again connects to application servers 28-30 though a network 26; however, the authentication engines 32 of Fig. 1 are co-located on a single authentication server 34. While suitable for its intended purpose, the client must still log into each of the application servers separately. Authentication occurs between the application servers and the authentication server for the client's establishment of a communications link.

Figure 3 illustrates another configuration wherein the clients 22-24 and application servers 28-30 are connected via the network 26 through an authentication server 36. In this instance the authentication server functions as a router in which the client 32 communicates to with each of the application servers through the authentication server 36 and can include a firewall 38 for security. While an improvement over existing authentication topologies, this authentication server can limit the client's access to the application by managing all communication between the client and the desired application server. In instances where a number of clients require communication the authentication server can delay communication between the application server and the client.

Thus, the need exists for a system for minimizing the authentication process across multiple servers in which authentication information can be distributed to multiple servers across a network.

SUMMARY OF THE INVENTION

The present invention is an automated authentication handling system that allows for a user to initiate a single authentication process with an authentication server that automatically handles the authentication of the user for all other servers across the network where the user is permitted access. The authentication server further establishes a trusted communication link between the user and at least one of the other servers.

The present invention can be more fully understood by reference to the following description and accompanying drawings, which form an integral part of this application:

BRIEF DESCRIPTION OF THE DRAWINGS

Figures 1-3 are functional block diagrams of typical client network connection topologies;
Figure 4 is a functional block diagram of a client network connection to application servers using an authentication server of the present invention;
Figure 5 is a functional block diagram of an authentication server having an identifier engine and a communication initiator engine; and
Figure 6 is a functional block diagram of a authentication signal flow during an authentication.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to Figure 4 for purposes of illustration, an automated authentication handling system 100 according to the present invention includes a plurality of clients 102-104 that are connected via a network 106 such as the Internet or an intranet. Similarly a plurality of application servers 108-110 are connected to the network. Advantageously the present invention includes an authentication server 111 connected to the network 106 and configured to authenticate the clients and application servers to establish a communication link 112-114 directly between the clients 102-104 and the application servers 108-110. For purposes of illustrating the features of this invention, the invention will be described in the context of the Internet protocols and more particularly the HyperText Transfer Protocols. However those skilled in the art will appreciate that the features of this invention may be utilized on any network protocol platform.

The authentication server 111 generally may include conventionally available hardware and software for connecting to the network and interacting with the network communication protocols used by the network. For example, when used over the Internet the server may include web server software of the type published by Apache Digital Corporation of Durango, CO. The Apache web server software is preferred as the server software may be easily configured to include specialized tasks using software compatible with the Common Gateway Interface (CGI). The authentication server of the present invention includes two specialized tasks or modules (Figure 5), namely, an identifier engine 116 and a communication initiation engine 118.

With continued reference to Figure 5, the identifier engine 116 includes a database 120 having a plurality of client identifier records 122 and a plurality of application server records 124. Each of the client identifier records is related to one or more of the application servers. The relationships of the client identifier records to the application servers is preferably tailored to the desired relationships between the clients 102-104 and the applications servers 108-110. The result of the relationships is that for each client identifier in the database a listing of application servers authorized by the client identifier may be generated in a report. When a client provides a client identifier, a report 126 is generated and sent to the client containing a listing of the application servers authenticated for access by the client identifier. The report is preferably generated in a hyper-text format such as the hyper-text markup language (HTML) used by the hyper-text transfer protocol (HTTP) which makes up a part of the Internet protocols. The hyper-text format is embedded with a link for each application server in the listing. The link addresses the communication initiator engine on the authentication server and includes a request to establish a communication link with associated application server. This request is preferably in the form of an HTML POST command in which the application server is provided in the hypertext document in an encrypted format. This prevents the temptation by the user at the client to modify the hypertext document to change the access privileges.

Accordingly, the hypertext report provides a user interface 128 that may be used by a client when the hypertext document is loaded by a conventional web browser of the type such as Explorer published by Microsoft or Navigator published by Netscape. The user interface 128 when used on a client having a conventional graphical user interface such as Microsoft Windows or Apple Macintosh OS, may appear as a separate window that can be accessed when needed by a user on the client. Using the HTML language it will be appreciated that a number of user interface configurations maybe used including, but not limited to, pull-down menus or hypertext listings. Once the document has been sent to the client, no further authentication by the user is required to access the application servers contained in the listing. This user interface provides a great advance over existing authentication methodologies as the user does not have to provide a separate authentication for each of the application servers. Furthermore, it will be appreciated that the authentication administration can be handled by a single server rather than having separate authentication administration for each of the application servers. The client's communication with the authentication may include a Secure Socket Layer (SSL) session link, cookies or other conventional security measures that may be used to verify continued communication from the client to the authentication server.

In another embodiment, the client identifier is further related to session assignment information for each of the application servers. The session assignment can include information for limiting client access to the features on each of the application servers as well as session timeout information. It will be appreciated that the session assignment information may be specifically tailored to the access capabilities of each of the application servers. When the report in hypertext format is sent to the client the link designating a request for an application server my be encoded with the application server information also in an encrypted format.

The communication initiator engine 118 is responsive to a request from the client to establish a communication link 130 with one of the application servers. The communication initiator engine 118 preferably receives the encrypted request information illustrated by line 132 and decrypts the information. The request information is preferably compared to a look-up table in which each application server and session assignment information is stored as a separate listing. The authentication server matches the client's request with the appropriate listing. The listing is combined with the client's address. The client address and the session information is then encrypted by the communication initiator engine and transmitted to the application server illustrated by line 134 again using the HTTP POST method.

The application server receives the information transmitted in the post command and includes a verification engine 136, preferably running as a CGI script on the application server. It should be noted that the verification engine 136 does not verify that the information was received by checking the IP address of a trusted authentication server, rather it decrypts the posted information and uses a shared secret data field to verify the authentication server. It will be appreciated by those skilled in the art that such verification allows for the dynamic IP addressing of the authentication server. The encryption/ decryption method used by the present invention may vary; however, a public key/ private key methodology is presently preferred.

Thus, the decryption of information from the authentication server is decrypted using the private key contained on the application server. The decrypted information includes the session assignment information and the client's address. The pushed information also preferably includes a verification record that contains secret information shared exclusively between the authentication server and the application as a further verification that the information was transmitted from a trusted source. If the verification fails an error message is returned and no further action is taken.

If the verification is cleared, a Uniform Resource Locator (URL) is generated containing a unique address for the client to access the application and further includes session assignment information that is encrypted by the verification engine prior to transmittal. The special URL is then transmitted to the Authentication Server illustrated by line 140 which in turn forwards the URL directly to the Client illustrated by line 142. Once received by the client, the URL is addressed back to the application server directly from the client along with the encrypted session information initiating the communication link 134. The application server again decrypts the session information and verifies that the URL request was transmitted from the IP address of the client 102 originally transmitted to the application server by the authentication server. The application server also verifies that the session timeout time is still valid. The application server then establishes the trusted communication link 134 directly with the client. The trusted communication link 134 may include security such as an SSL communications link or a cookie containing the relevant session information may be placed on the client's computer. The cookie is used by the application to verify the user and provide other information relevant to the session such as a session time-out information. The URL then redirects the Client to the main session application page of the web site.

With reference to Figure 6, the signaling between a client 102 and an application server 108 using an authentication server 108 includes initiating a login request from the client to the authentication server illustrated by line 125. The authentication server replies with a report in hypertext listing the application servers authorized access by the client illustrated by line 126. A client selects an application server for access and submits a request to the authentication server illustrated by line 132. The authentication server forwards the request to the application sereer illustrated by line 134. The application server responds and confirms access as illustrated by line 140. The authentication server forwards the selection authorization to the client 102 illustrated by line 142. The client 102 and application server 108 establish and communicate via a trusted communication link illustrated by line 130.

It is understood that the above description and drawings are illustrative of the present invention and details contained therein are not to be construed as limitations on the present invention. Changes in procedure and structure may be made without departing from the scope of the present invention as defined in the following claims.

WHAT IS CLAIMED IS:

1. An automated authentication handling system for use by clients on a network comprising:

a plurality of application servers connected to said network, each requiring authentication for access; and

an authentication server adapted to authenticate at least one of said clients and establish a trusted communication link for access by an authenticated user to at least one of said application servers.

2. The automated authentication handling system of claim 1 wherein said authentication server includes:

an identification engine configured to maintain collections of session assignments for accessing said application servers, each of said session assignment collections being associated with a client identifier.

3. The automated authentication handling system of claim 2 wherein said identification engine is adapted to receive client identifiers from said clients to establish authenticated users and responsive thereto to provide a user interface to access said application servers according to said associated session assignments.

4. The automated authentication handling system of claim 1 wherein said authentication server includes:

a communication initiator engine configured to establish a trusted communication link between said authenticated users and said application servers.

5. The automated authentication handling system of claim 3 wherein said authentication server includes:

a communication initiator engine configured to establish a trusted communication link defined to one of said session assignments between said authenticated users and said application servers.

6. The automated authentication handling system of claim 1 wherein said session assignments include data fields selected from the group consisting of session timeout and application access level.

7. The automated authentication handling system of claim 1 wherein said client identifiers include a user id and password.

8. The automated authentication handling system of claim 1 wherein said authentication server includes a processor under the control of software to:

receive an authentication signal from said client;

provide an application access interface to said client in response to said authentication signal; and

establish a trusted communication link between said client and a application server selected from said application access interface.

9. A method for automatically authenticating a client for a plurality of application servers comprising the steps of:

providing an authentication server;

identifying clients for access to said application servers by said authentication server; and

establishing a trusted communication link between at least one of said clients and at least one of said application servers.

10. The method of claim 9 wherein said identifying step includes:

providing a session parameters for each of said identified clients for at least one of said application servers.

11. The method of claim 9 wherein said identifying step includes:

providing a user interface to said identified clients for accessing said application servers.

12. The method of claim 10 wherein said establishing step includes:

using said session parameters to establish said trusted communication link.

13. The method of claim 11 wherein said user interface includes a listing of application servers and said establishing step is initiated following a selection of an application server by a user from said user interface.

ABSTRACT

An automated authentication handling system for use by clients on a network including a plurality of application servers connected to the network, each requiring authentication for access and an authentication server adapted to authenticate at least one of the clients and establish a trusted communication link for access by an authenticated user to at least one of the application servers.

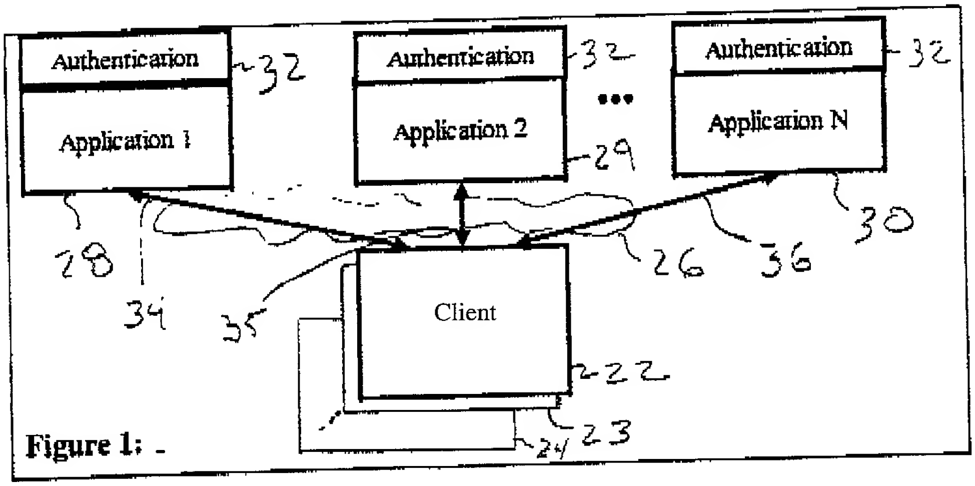

Figure 1:

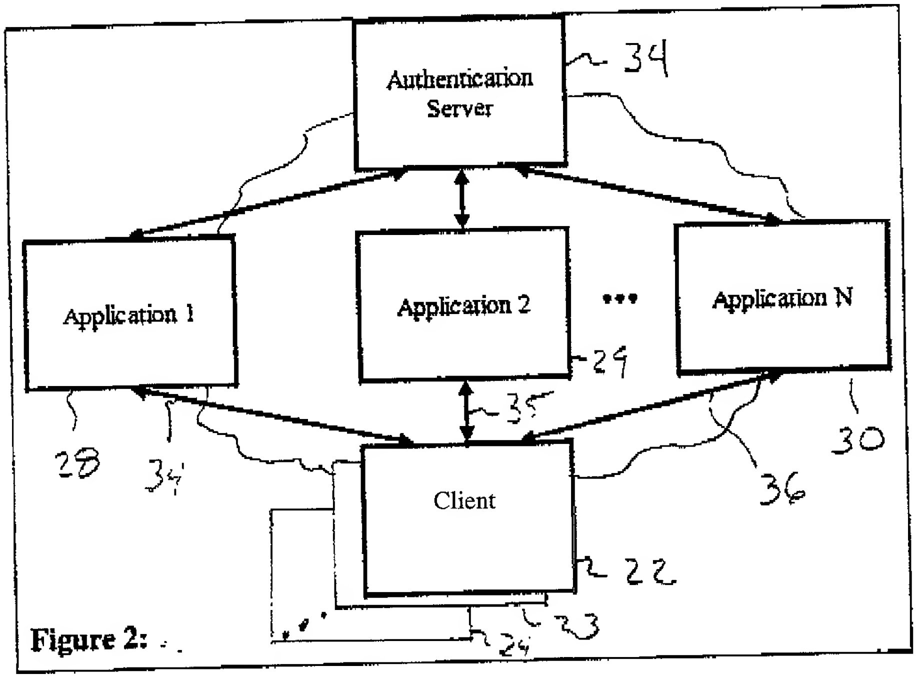

Figure 2:

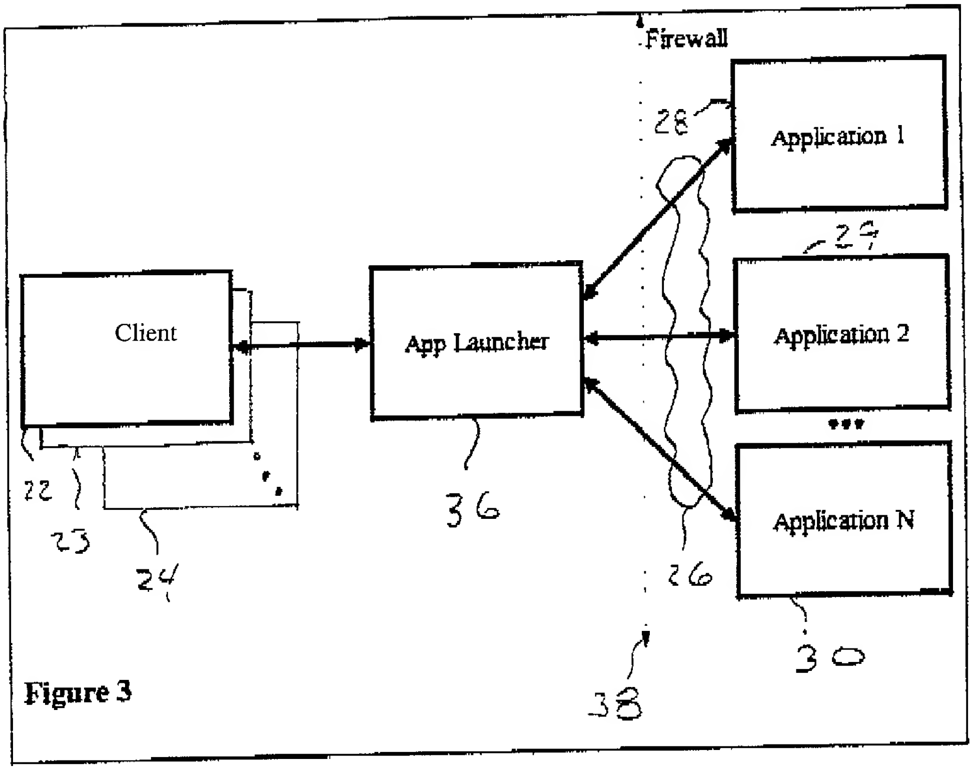

Figure 3

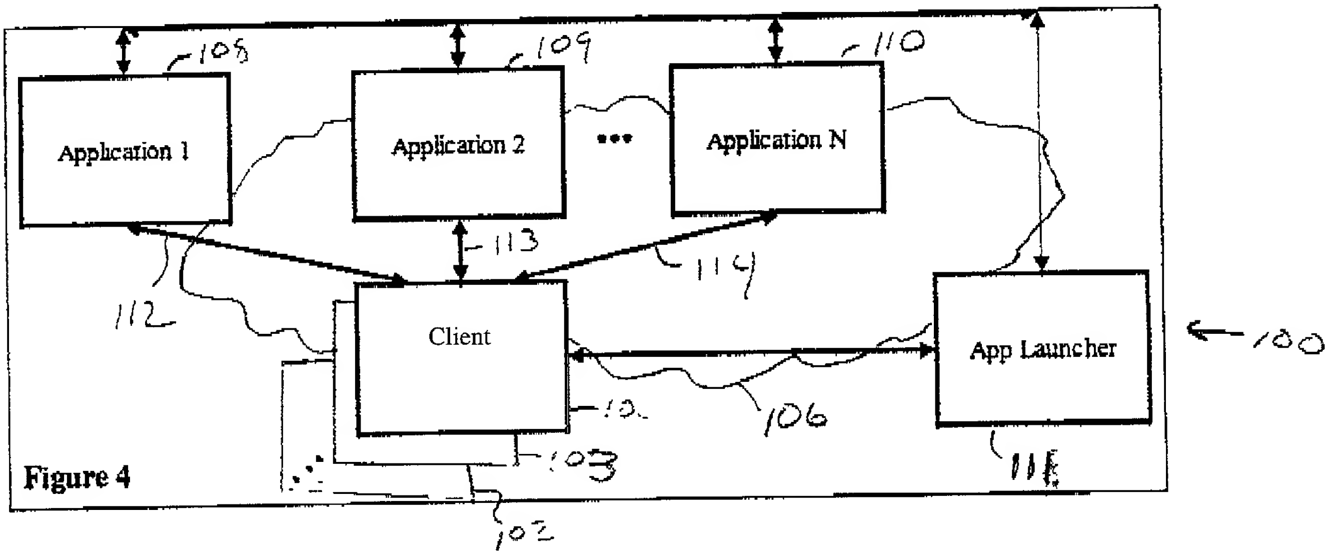

Figure 4

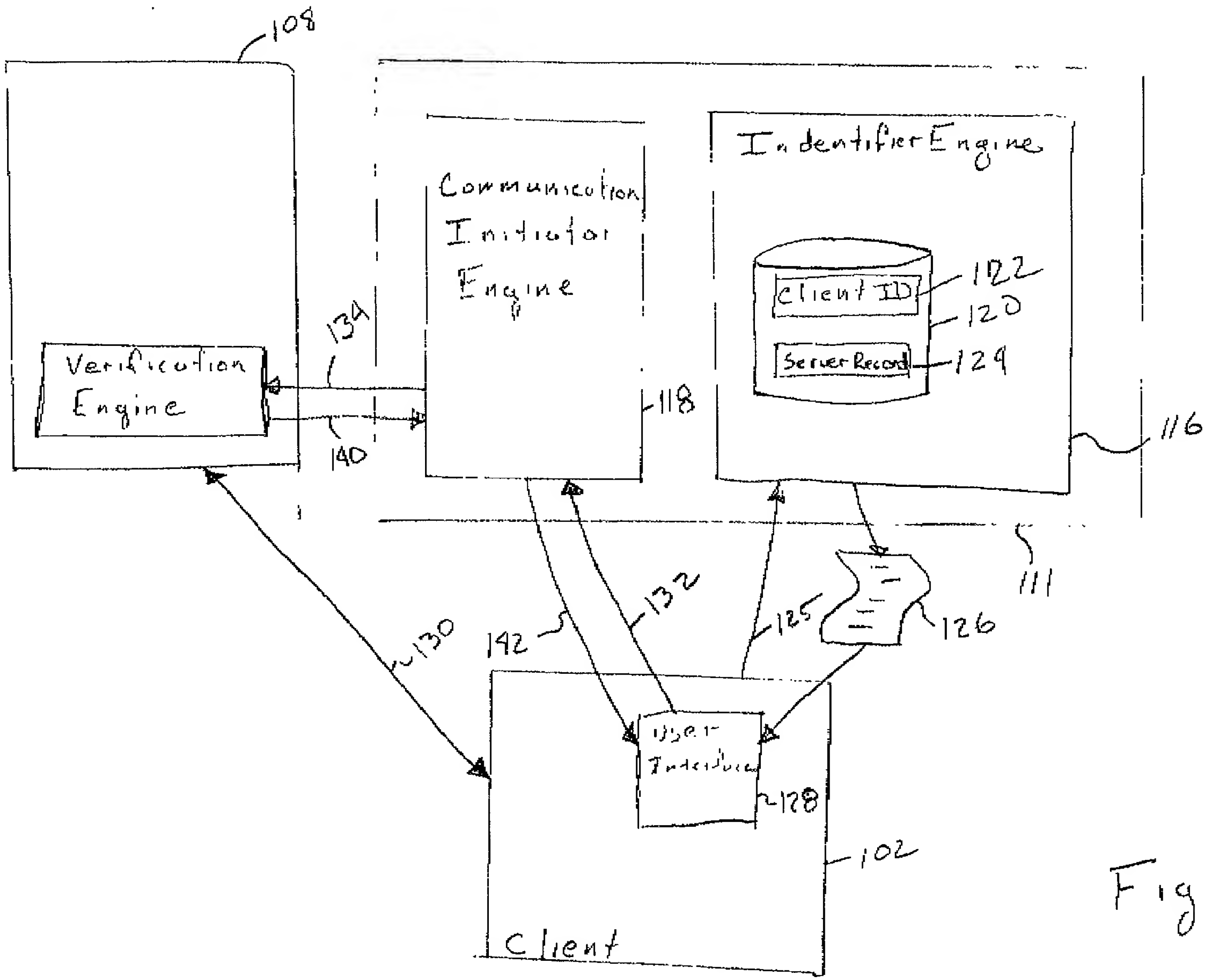
108
Verification Engine
134
140
Communication Initiator Engine
118
Indentifier Engine
Client ID
Server Record
122
120
129
116
111
126
125
132
142
130
User Interface
128
102
Client

Fig 5

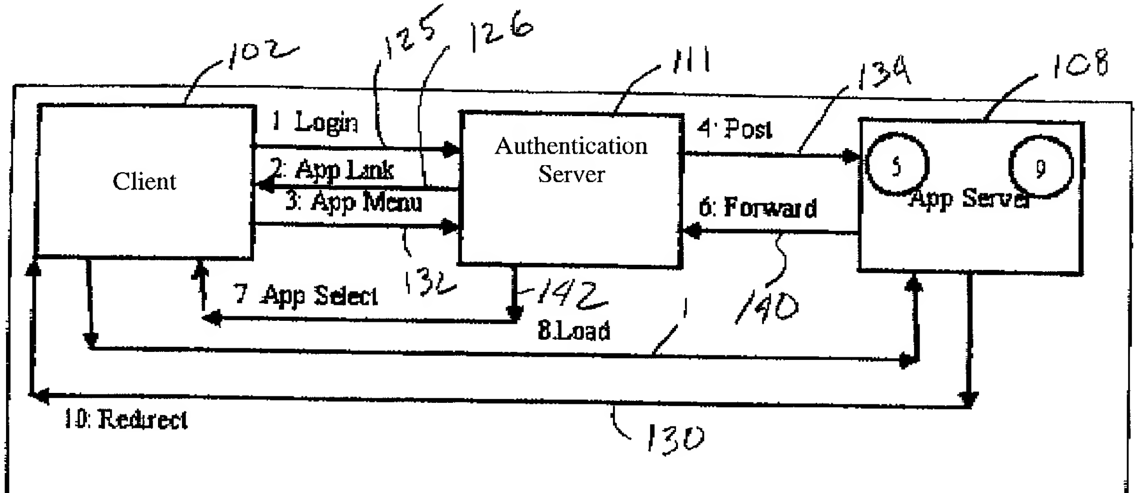
102
125
126
111
134
108
Client
1 Login
2: App Link
3: App Menu
Authentication Server
4: Post
6: Forward
5
9
App Server
7 App Select
132
142
140
8.Load
10: Redirect
130

Figure 6

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our name.

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled **AUTOMATED AUTHENTICATION HANDLING SYSTEM** filed herewith.

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

We acknowledge the duty to disclose all information known to us which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

We hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None.

We hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, we acknowledge the duty to disclose all information known to us to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

We hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
Donald P. Dinella	(Reg. No. 39961)
Guy Eriksen	(Reg. No. 41736)
Martin I. Finston	(Reg. No. 31613)
William S. Francos	(Reg. No. 38456)
Barry H. Freedman	(Reg. No. 26166)
Julio A. Garceran	(Reg. No. 37138)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
Stephen M. Gurey	(Reg. No. 27336)
John M. Harman	(Reg. No. 38173)
Matthew J. Hodulik	(Reg. No. 36,164
John B. MacIntyre	(Reg. No. 41,170)
Michael B. Johannesen	(Reg. No. 35557)
Mark A. Kurisko	(Reg. No. 38944)
Irena Lager	(Reg. No. 39260)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Martin G. Meder	(Reg. No. 34674)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Joseph J. Opalach	(Reg. No. 36229)
Neil R. Ormos	(Reg. No. 35309)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Gregory C. Ranieri	(Reg. No. 29695)
Scott J. Rittman	(Reg. No. 39010)
Ferdinand M. Romano	(Reg. No. 32,752)
Ozer M.N. Teitelbaum	(Reg. No. 36,698)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
John P. Veschi	(Reg. No. 39058)
David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Jeffrey M. Weinick	(Reg. No. 36304)
Eli Weiss	(Reg. No. 17765)

We hereby appoint the attorney(s) on ATTACHMENT A as associate attorney(s) in the aforementioned application, with full power solely to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected with the prosecution of said application. No other powers are granted to such associate attorney(s) and such associate attorney(s) are specifically denied any power of substitution or revocation.

Full name 1st joint inventor: Carl Bilicksa

Inventor's signature Carl Date 9/29/2000

Residence: 3 Jacobus Lane
Readington, NJ 08822

Citizenship: USA

Post Office Address: 3 Jacobus Lane
Flemington, NJ 08822

Full name 2nd joint inventor: Douglas Allen Sisk

Inventor's signature ______________________ Date 9/29/00

Residence: 15 Wharton Way
High Bridge, New Jersey 08829

Citizenship: USA

Post Office Address: 15 Wharton Way
High Bridge, New Jersey 08829

ATTACHMENT A

Attorney Name(s):	Henry J. Walsh	Reg. No.:	24,451
	Roger Rathbun		24,964
	David Padnes		28,384
	David J. Rosenblum		37,709
	Donald J. Cox		37,804
	Kristine L. Butler		42,376
	Vincent E. McGeary		42,862

Telephone calls should be made to **Donald J. Cox, Jr., Esq. at Gibbons, Del Deo, Dolan, Griffinger & Vecchione** at:

Phone No.: 973-596-4500 or 973-596-4853

Fax No.: 973-596-6368

All written communications are to be addressed to:

Intellectual Property Docket Administrator
Gibbons, Del Deo, Dolan, Griffinger & Vecchione
One Riverfront Plaza, Newark, New Jersey 07105-5497